Weekly Report

2016.0801-2016.0807

1 This Week

Security Project

1. Revise the biding document.
2. Prepare for the school materials for the biding document.
3. Contact with the other two companion company.
4. Prepare for the technical documents for the other two companion company.

2016 VIS Poster

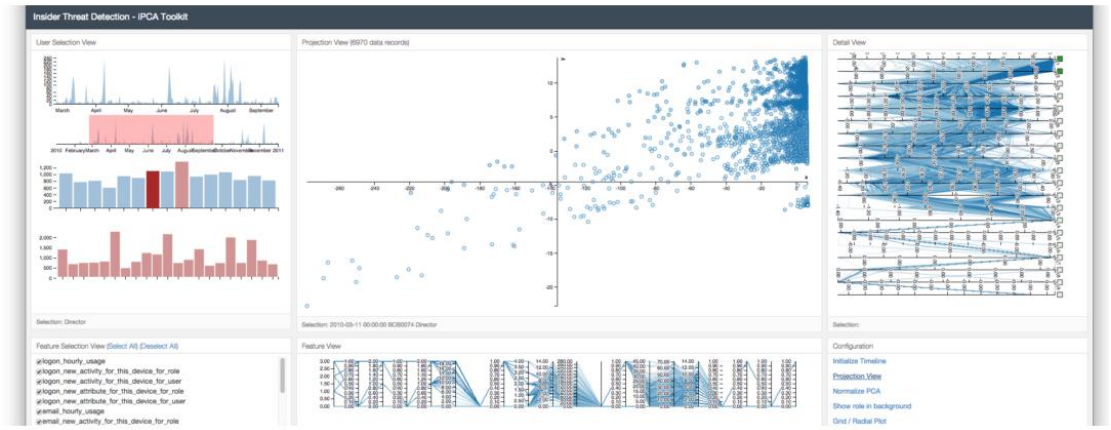
1. Design and make the poster 25 second video of Structural Hole Spanner with Guo.

Friday Group Meeting

1. Attend the group meeting and share thoughts with other group members.

Paper Reading

1. **Visualizing the Insider Threat: Challenges and tools for identifying malicious user activity**

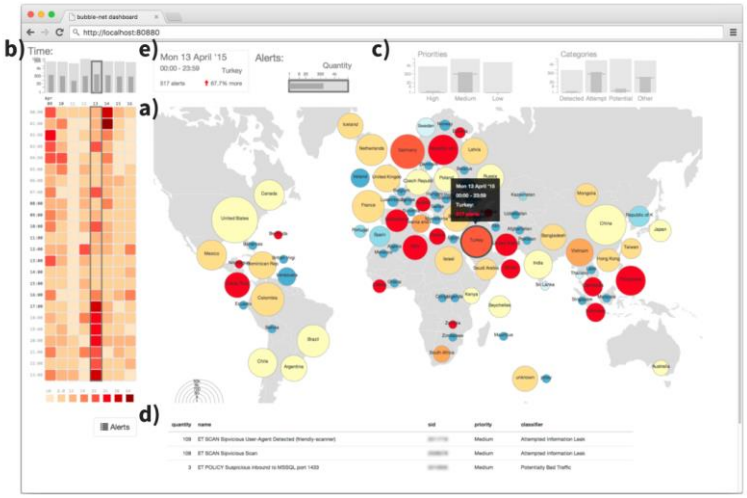


This paper employs the Carnegie Mellon University CERT Insider Threat Dataset and present a visual analytics approach that incorporates multiple views to detect and analyze malicious insiders activities. There are three main interesting parts of this paper:

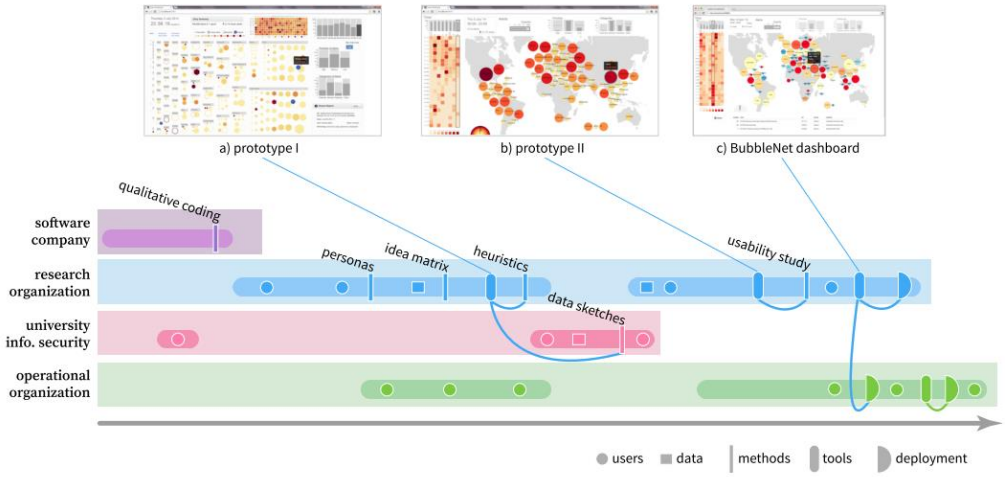
1. They define malicious insider behavior based on the roles of the insider. Only those strange activities against their role will be considered malicious.
2. The introduction of the system part in this paper is organized following the Information-Seeking mantra.

3. The scatter plot in the system is based on interactive PCA. The analyst is able to select and drag points. Once a point is dragged, the serve computes an inverse PCA transformation based on the original model, to map the new position back to the original feature space. This allows the analyst to clearly understand the contribution that each feature has on the output of the PCA metric that supports reasoning as to why a user appears as an anomaly.

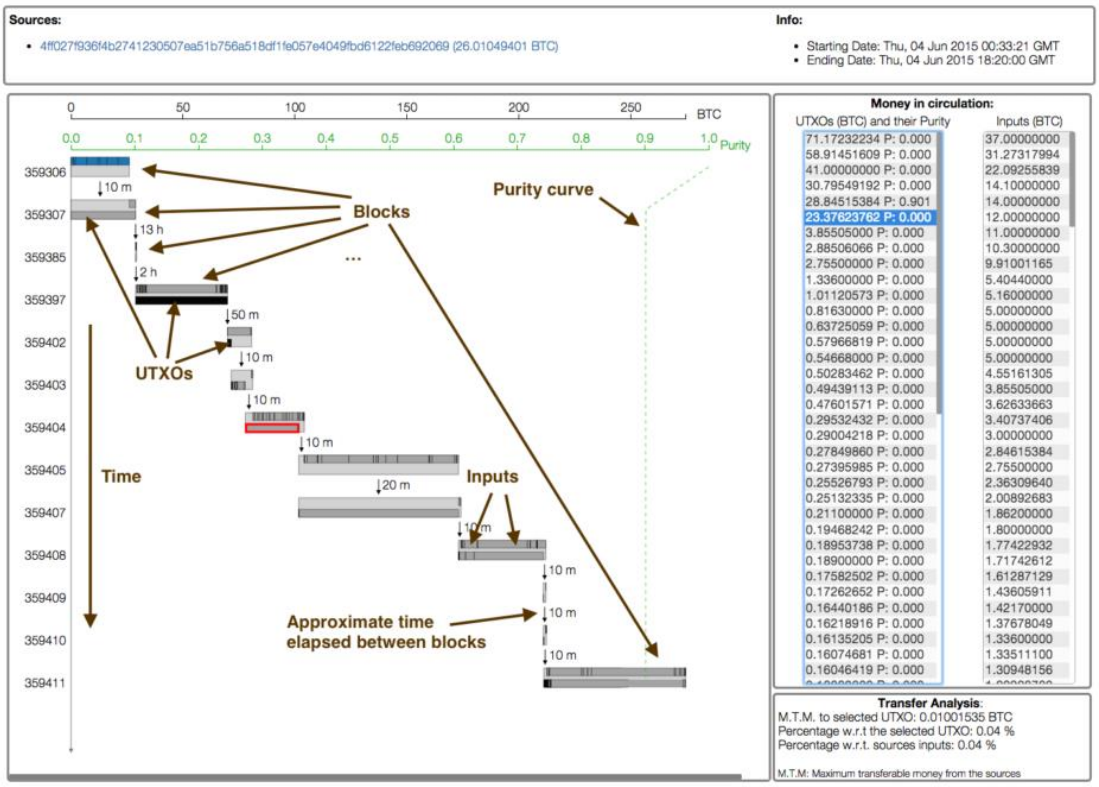
2. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns



This paper focus on the task of discovering and presenting cyber security patterns. It' s main visualization design is quite simple: the location view uses circles to indicate records of each single country (very similar to force directed layout); the temporal view uses a bar chart and a heat map to show patterns of each week, each day, and even each hour.
Although the visualization is not good enough, the design process of this paper does give us an indication about how to co-operate with people beyond data analysis.



3. Bitconeview: visualization of flows in the bitcoin transaction graph



This paper presents a system for the visual analysis of Bitcoin flows in the blockchain. It mainly focuses on detecting mixing processes and patterns.

The timeline flows from top to bottom. Each block is represented by a rectangular region filled in light gray. Such a rectangular region provides a compact representation of the subgraph of interest by aggregating all transactions that fall into the same block.

Visualization here is not aesthetic but useful for representing financial transactions with bitcoins. However, this design is not efficient for the reason of space wasting. Better visualizations need to be discovered for transaction chains.

2 TODO

1. Preparing biding documents for the security project.
2. Keep on the coding part of the security project and revise bugs.
3. Write Zongzhuang’ s survey.